(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number
WO 01/30036 A1

(51) International Patent Classification[7]: H04L 12/64, 29/06

(21) International Application Number: PCT/NO00/00336

(22) International Filing Date: 11 October 2000 (11.10.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
19995081 18 October 1999 (18.10.1999) NO

(71) Applicant *(for all designated States except US)*: TELEFONAKTIEBOLAGET L.M. ERICSSON [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BACH CORNELIUSSEN, Knut, Snorre [NO/NO]; Bygdøy Allé 117A, N-0273 Oslo (NO). KLILAND, Kevin [NO/NO]; Finstadsvingen 11, N-1400 Ski (NO).

(74) Agent: WESMANN, Johan, Fredrik; Bryns Patentkontor A/S, P.O. Box 765, Sentrum, N-0106 Oslo (NO).

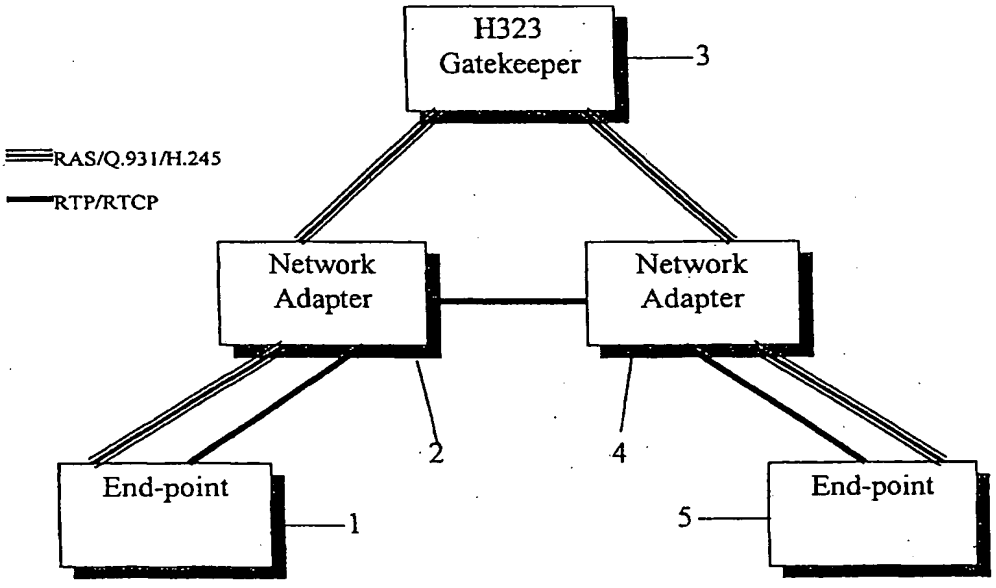
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AN ARRANGEMENT FOR H.323 PROXIES



(57) Abstract: The invention provides, in multimedia networks comprising firewalls, an arrangement for a communications unit, especially for H.323 proxies, whereby a network adapter (NA) (2, 4) is provided. The NA (2, 4) provides mechanisms for letting multimedia H.323 traffic through firewalls and a wide range of functionalities such as firewall support, NAT, media stream multiplexing, QoS mechanisms, performance enhancements for signalling connections, eavesdropping, bridging, interacting with media channels, and integrity, authentication and privacy between network adapters of the invention.

WO 01/30036 A1

AN ARRANGEMENT FOR H.323 PROXIES

FIELD OF THE INVENTION.

The present invention relates to large scale multimedia network implementations according to the H.323 standard recommendation of the International Telecommunication Union, and especially to such networks comprising firewalls.

THE PROBLEM AREAS.

The recommended standard H.323 describes multimedia networks and communication therein, wherein such networks may include local area networks (LAN) such as a LAN in a private enterprise, a public agency, a business corporation or some other type of organisation. In order to protect a LAN connected to other networks from unauthorised, and possibly hostile access from network users outside the LAN, communication between the LAN and other networks is often run through a protection arrangement referred to as a firewall. The firewall interacts with the communication so as to limit or refuse undesired or unwanted communication according to a given set of rules.

Important areas covered by H.323 are:

a) Registration, admission and status (RAS) signalling,

b) Q.931 and H.245 signalling, and

c) traffic and media channels

RAS is usually signalled over predefined ports and is accordingly trivial to get through firewalls. Q.931 and H.245 are usually signalled over dynamically allocated ports and hence more difficult to get through firewalls. In a H.323 Gatekeeper (GK) routed call, such as when two endpoints communicate via a GK and not directly, a GK in some way has to interact with a firewall in order to let such traffic through. It is however even more difficult to let the media channels through firewalls as such traffic is normally set up directly between the endpoints. This means that an arrangement comprising a GK in some way interacting with a firewall and the endpoints and or a corresponding arrangement has to be made.

Performance improvements e.g. by multiplexing traffic, prioritising traffic or QoS (Quality of Service), eavesdropping, interfering with the media (e.g. for adding commercials) and bridging (e.g. between protocols and or protocol versions), security

mechanisms (integrity, authentication and privacy) all points out functionality normally hard to achieve in H.323 networks.

KNOWN SOLUTIONS AND PROBLEMS WITH THESE.

One known solution to the problems described above is to use proprietary endpoints and firewalls. This still do not solve problems related to let H.323 traffic through firewalls, traffic prioritising, Quality of Service and security mechanisms.

Another known solution for letting the media and signalling channels through a firewall is to open a wide range of ports for User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) traffic. A serious disadvantage of such a solution is that the firewall then has practically no control of the traffic going into the LAN which it is supposed to protect.

Further, security mechanisms for purposes such as integrity, authentication and privacy might be achieved and supported by the endpoints themselves. Disadvantages of those solutions are that they might spend some extra time on negotiation the security properties, and that other standards or conventions have to be deployed and supported. Especially on UDP, which is the media traffic bearer, Internet Protocol Security (IPSEC) that might support e.g. media channel privacy is of little value as it is not deployed on a sufficient scale.

Further background material related to the technical area is presented in a number of patent related documents: US 5 802 058 which discloses a media manager in a communications network that intermediates connection setup between endpoints and marshals resources for the connection; WO 98/37664 describes a network wherein a set of media components including IP traffic is encapsulated in an ATM VC as an entity and switched using a robust signalling system to employ resultant connection records for usage based tarriffing; and US 5 898 830 discloses a firewall providing enhanced network security and user transparency.

Mechanisms for letting H.323 traffic through firewalls by providing some kind of proxy arrangement exist and are also known. Problems in these mechanisms are related to "fast start" and "tunneling", and the fact that the elements endpoints, proxy and gatekeeper all need to cooperate and interact with each other for solving the problem.

OBJECTS OF THE INVENTION.

Accordingly, it is an object of the present invention is to propose an arrangement which is capable of solving all of the problems mentioned in the Problem Areas section of this specification.

BRIEF DISCLOSURE OF THE INVENTION.

The objects of the present invention is achieved by providing an H.323 proxy, hereinafter referred to as a network adapter (NA), which could be embodied by implementation as a small computer application. The NA is typically located somewhere on the LAN or the border of corporate LAN, and usually in the demilitarised zone (DMZ) of a firewall. The network adapter of the present invention is capable of solving all of the problems mentioned in the Problem Areas section of this specification. The network adapter receives all the signalling (RAS/Q.931/H.245 hence is itself a GK) as well as the media (RTP/RTCP) from its connected endpoints, other network adapters and/or one or more H.323 gatekeepers (GK). A description of the signalling and the media traffic is given in a later section of this specification.

BRIEF DESCRIPTION OF THE DRAWINGS.

Figure A is a schematic drawing of an example a possible configuration of a multimedia network incorporating the network adapter of the present invention, and figure B is a schematic drawing of a network adapter of the present invention.

DETAILED DESCRIPTION OF EMBODIMENTS.

With reference to figure 1, an example of a typical signalling scenario is shown, wherein an endpoint (1) behind a NA (2) is communicating with another endpoint (5) behind another NA (4), and wherein both NAs are communicating with the same GK (3) . The same signalling scenario could also be described by:

endpoint (1) -> network adapter (2) -> gatekeeper (3) -> network adapter (4) -> endpoint (5).

Media follows to some extent the same path, but is in the example of figure 1 communicated directly between the two network adapters NA (2) and NA (4) respectively.

The network configuration regarding the locations of the endpoints, NAs and GKs could however be arranged in various ways, also different from the example shown in figure 1.

The important features of a network adapter of the present invention are:

a) Endpoints need not be made aware of the fact that its traffic is passed through a network adapter.

b) There is no constraint on the number of network adapters that could forward traffic between endpoints.

Referring to figure 2, a network adapter consisting of two different modules is shown. One module is a controlling part (6) for controlling the H.323 signalling (RAS/Q.931/H.245) and another is a forwarding part (7) for forwarding media packets.

The controlling module or part (6) is responsible for communicating with endpoints, gatekeepers and other network adapters. It is also responsible for providing instructions to the forwarding part regarding where to expect traffic, and to where this traffic should be sent.

The forwarding module or part (7) simply forwards media traffic from a NA port connected to an H.323 client to a NA port connected to another NA. Hence this part is a prerequisite when traversing firewalls. Since the forwarding part also handles TCP, T.120 is supported also for the T.120 clients dynamically allocating ports

The NA of the present invention is contemplated also to include functionality such as:

a) Enabling of support for firewalls and Network Address Translation (NAT). When controlling both the signalling and media, the network adapter of the present invention can use the H.245 part of H.323 to instruct endpoints and NAs on which port and IP address to send traffic. When controlling where the endpoints and NAs of the present invention receive and send its media, it is simple to configure a firewall to support this arrangement by opening a predefined range of ports. When enabling endpoints located in different NAT to communicate with H.323, the network adapters of the present invention should be placed in a De-Militarised Zone (DMZ). The F-interface (8), as shown in figure 2, is used by the controlling part for instructing the forwarding part on which connections to forward traffic, as described earlier.

b) Multiplexing of several media streams going to the same receiving network. By multiplexing H.323 traffic among network adapters, this traffic can be sent on separate underlying links or virtual connections. Such connections might have

different QoS. By multiplexing is meant transmitting several media streams, otherwise sent on separate UDP connections, on the same UDP connection. Accordingly, a multiplexing protocol must include some sort of original connection identity on the multiplexed UDP connection. This functionality will be provided by the controlling part

c) Implementing other QoS mechanisms. This could be achieved by first determining the round trip delay, such as by sending test probes or packets from a NA towards another identified NA, or by other means. Then, if the round trip delay is deemed to be too high, the NA could refuse a connection on a set-up attempt. Such functionality will be provided by the controlling part and may be used when setting up new connections

d) Multiplexing of the signalling connections in order to enhance performance. This requires a signalling multiplexing protocol that could work in the same way as a media multiplexing protocol, although on TCP instead of UDP. This functionality is provided by the controlling part.

e) Provision of integrity, authentication and privacy can easily be applied between network adapters. For such purposes, IPSEC and or SSL may be applied. A configuration manager may decide the kind of security mechanisms which is to apply between different NAs. As an example, SSL could be used for all TCP (used for signalling) connections between certain identified GKs and NAs. A manager may specify that between certain identified NAs, IPSEC shall be used on all UDP connections. This functionality can be provided by the controlling or the forwarding part, or by a combination of these.

f) Eavesdropping. Because all media traffic is routed through the network adapter, eavesdropping can be performed at this point. Eavesdropping of H.323 communications that does not go through a network adapter is generally difficult, because you have no control over where the traffic is flowing, or of which set of ports are used for H.323 media. However, in the NA of the present invention, implementation of support for eavesdropping is simple. The controlling part, the F-interface and the forwarding part makes use of methods for copying UDP packets on certain predefined connections, and then forward such copies to a recording unit.

g) Support for local differences from H.323. Different kinds of bridging can be located in the network adapter of the present invention. Such bridging may be to translate between different versions of the standard, such as version 1 of h.323 to version 2, or

between different standards, such as SIP to H323. This functionality may be provided by the controlling or the forwarding part, or a combination of these.

h) Interacting with the media channels by means of a media Application Programmers Interface (API), located above the forwarding part. Commercials and advertising may easily be applied in this way. This may be accomplished in different ways, such as by replacing or combining certain parts of a video conference with commercial text or video, or a combination of these. Such a media API must have possibilities for specifying where to perform such replacing and what to replace with. This is a rather complex task, since knowledge or information of parameters such as the video format etc. must be obtainable. Such information may, however, be obtained from and by means of the signalling or the controlling part. Hence an arrangement supporting such functionality has to be provided by both the controlling part and the forwarding part. In this context, another possibility provided by the NA of the present invention, is the possibility to add an identity of a person or persons taking part in a video conference. This information would also have to be obtained from and by means of the controlling part, by reading the end-user alias (typically E.164 number or e-mail alias), and then insert the identity information somewhere in the video conference picture.

It should be noted that all of the mechanisms and functionality described above may be applied on any network providing media.

Now, again with reference to figure 2, in the following, an example of an implementation of a F-interface (8) between a controlling part (6) and a forwarding part (7) of a network adapter according to the present invention is described:

The forwarding part (7) provides an interface with three basic commands or messages and their corresponding acknowledge messages and return values:

a) *openChannel(direction, protocol) -> return freePort, status*(ok/not ok)

b) *startChannel(direction, port, remoteIpAddress, remotePort, protocol) -> return status* (ok/not ok)

c) *closeChannel(port, direction, protocol) -> return status* (ok/not ok)

The parameter *direction*, indicates either from the LAN environment to the external environment or from the external environment to the LAN environment. The parameter *protocol* is either TCP or UDP, indicating that the network adapter example according to the present invention is also supporting TCP packets forwarding, although initially built to forward UDP packets.

In the example described above, the reason for separating *openChannel* and *startChannel* was to optimise the code. The message *openChannel* initiates and sets up parts of the environment that may be initiated and prepared before the *startChannel* command is executed, such as for getting a free server port etc.

The H.323 message that triggers both the *openChannel* and *startChannel* messages is the Q.931 set-up message when running fast start, and the H.245 openLogicalChannel message when running plain H.323. On closing, it is in order the Q.931 releaseComplete and H.245 closeLogicalChannel that invokes *closeChannel*. This applies in both cases when running TCP and UDP. To clarify, when running fast start, the H.245 openLogicalChannel is in fact tunnelled within the Q.931 set-up message. The *openChannel* and *startChannel* messages could in this scenario have been merged, but have, however, in other scenarios proven useful to be kept separate.

The network adapter comprises functionality for allowing signals/messages to traverse several nodes. A node can be an endpoint, a NA (network adapter) or a gatekeeper (in SIP, a SIP server). In a network, there may be several endpoints, gatekeepers (SIP servers) and NAs, i.e., both on the originating and the terminating side. Plain e.g. H.323 systems don't have such functionality, but this is provided in systems including the NA according to the invention. Two different solutions or approaches can support node traversal:

1. Either each node stores such information, preferably persistent; or

2. The signals/messages are updated with such information as the messages are transported through the system, and, hence, through NAs.

The type of information that has to be addressed is such as:

a) Addresses: Each node, or the message itself, must maintain data on which node that sent a message and to which node the message is going to be passed.

b) Endpoint or endpoint-like data: The home environment, represented by an H.323 gatekeeper (or SIP server) in this document, receives endpoint and or network adapter like information. NA like information might be accesstype (e.g. H323Phone, H323Pc PstnUni, PstnNni, H320Uni, H320Nni, GsmUni, GsmNni, PbxUni). Or similarly, for SIP systems, SipPhone, SipPc, etc..

If the message itself is going to maintain information on addresses, the following elements are added in the messages:

1. Address pair list: Each node in the system adds its addresses to the address pair list. There might in fact be several addresses for each node: The physical address of the node, the address of the voice channel, the media channel,etc.

2. Link index: The link index identifies which node is currently addressed in the address pair list. Messages can be issued either from the endpoints or the home environment gatekeepers. The link index only has to be used when messages are issued from the home environment gatekeepers. Then, the whole addressing path down to the endpoint should be included in the messages before the message traverse down to the endpoint. On the way, only the link index is modified.

The range of ports that the forwarding part of the NA is going to use has to be configured both on the firewall and the NA.

ADVANTAGES.

Important advantages provided by the NA of the present invention are:

- Firewalls can be traversed transparent to standard H.323 clients;
- NAT is supported;
- eavesdropping may be applied;
- commercials or advertising may be added;
- QoS mechanisms may easily be applied;
- performance improvements regarding both signalling traffic and media traffic by introducing multiplexing protocols may be achieved;
- bridging between different protocols etc. may easily be applied;
- security functionality may easily be added;
- due to that the forwarding part also handles TCP, T.120 is supported also for the T.120 clients dynamically allocating ports; and
- broadening can be achieved, wherein the forwarding part of the network adapter may be utilised by non-H.323 applications.

Acronyms:

DMZ	De Militarised Zone
GK	Gatekeeper
IPSEC	Internet Protocol Security
NA	Network Adapter
LAN	Local Area Network

Patent claims.

1.
An arrangement for a communications unit, especially for H.323 proxies, characterised in
a network adapter (2,4), the network adapter (2,4) comprising a controlling part (6) and a forwarding part (7), wherein
the controlling part (6) and the communicating part (7) are interconnected (8),
the controlling part is adapted to receive H.323 signalling, and
the forwarding part is adapted to receive media traffic.

2.
An arrangement according to claim 1, characterised in that the H.323 signalling comprises RAS, Q.931 or H.245 or any combinations of these.

3.
An arrangement according to claim 1 or 2, characterised in that the controlling part is adapted to communicate with endpoints, gatekeepers and other network adapters.

4.
An arrangement according to any of the previous claims, characterised in that the forwarding part is adapted to forward media traffic from a port of the network adapter connected to a client to a port of the network adapter connected to a port of another network adapter, and vice versa.

5.
An arrangement according to claim 4, characterised in that media traffic on a media channel is RTP or UDP.

6.
An arrangement according to any of the previous claims, characterised in that the network adapter is located in the demilitarised zone (DMZ) of a firewall.

7.
An arrangement according to any of the previous claims, characterised in that the network adapter is a gatekeeper.

8.

An arrangement according to any of the previous claims, c h a r a c t e r i s e d i n that the interconnection between the controlling part and the forwarding part conveys at least commands and messages selected from a group comprising: openChannel(direction,protocol) , returnfreePortstatus(status) , startChannel(direction,port,remoteIPaddress,remotePort,protocol) , returnStatus(status) and closeChannel(port,direction,protocol).

9.

An arrangement according to any of the previous claims, c h a r a c t e r i s e d i n that the network adapter provides functionalities of firewall support, NAT, media stream multiplexing, QoS mechanisms, performance enhancements for signalling connections, eavesdropping, bridging, interacting with media channels, and integrity, authentication and privacy between network adapters or a combination of one ore more of the aforementioned.

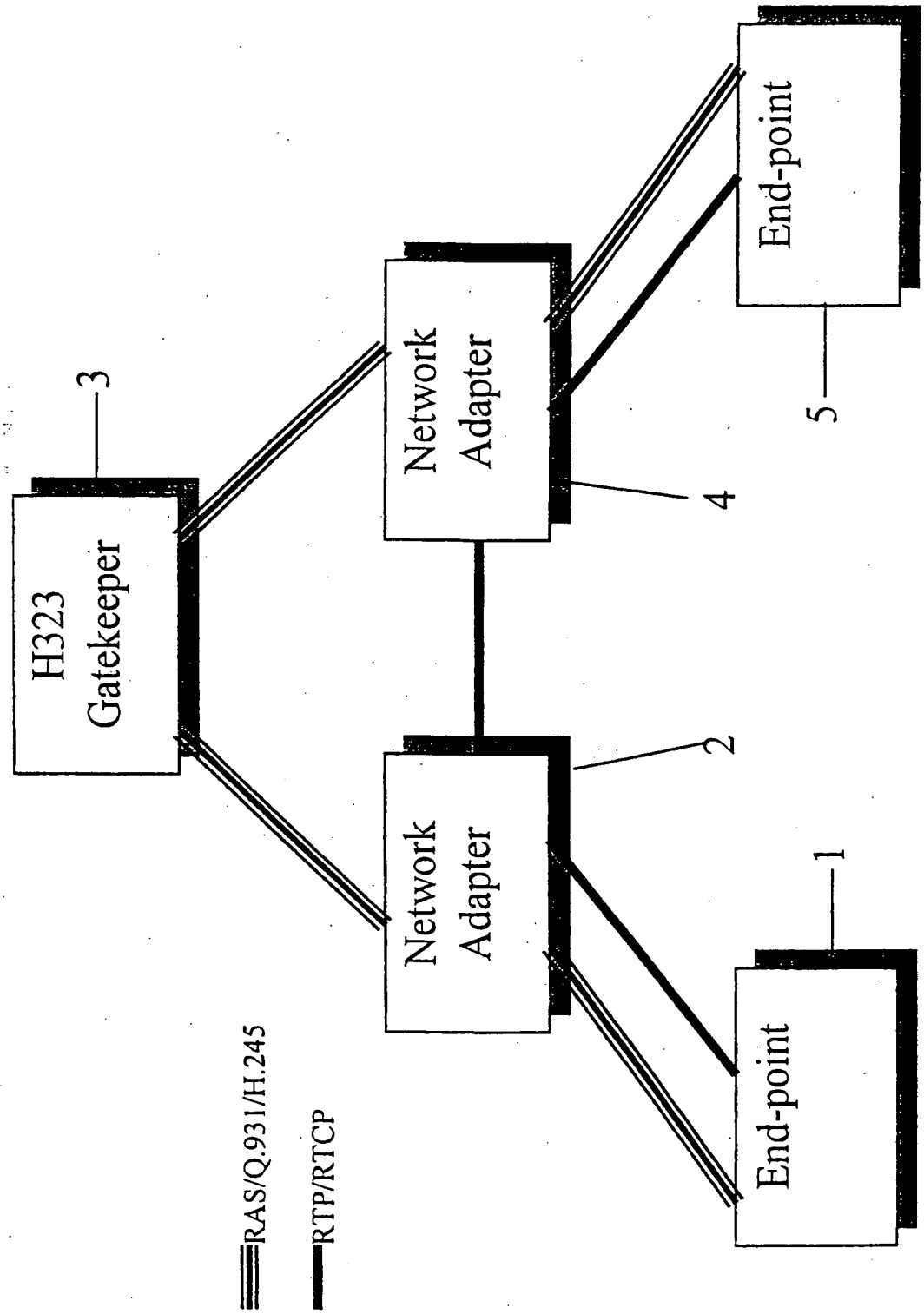

H323
Gatekeeper
3
Network
Adapter
Network
Adapter
2
4
End-point
5
End-point
1
RAS/Q.931/H.245
RTP/RTCP

Fig. 1

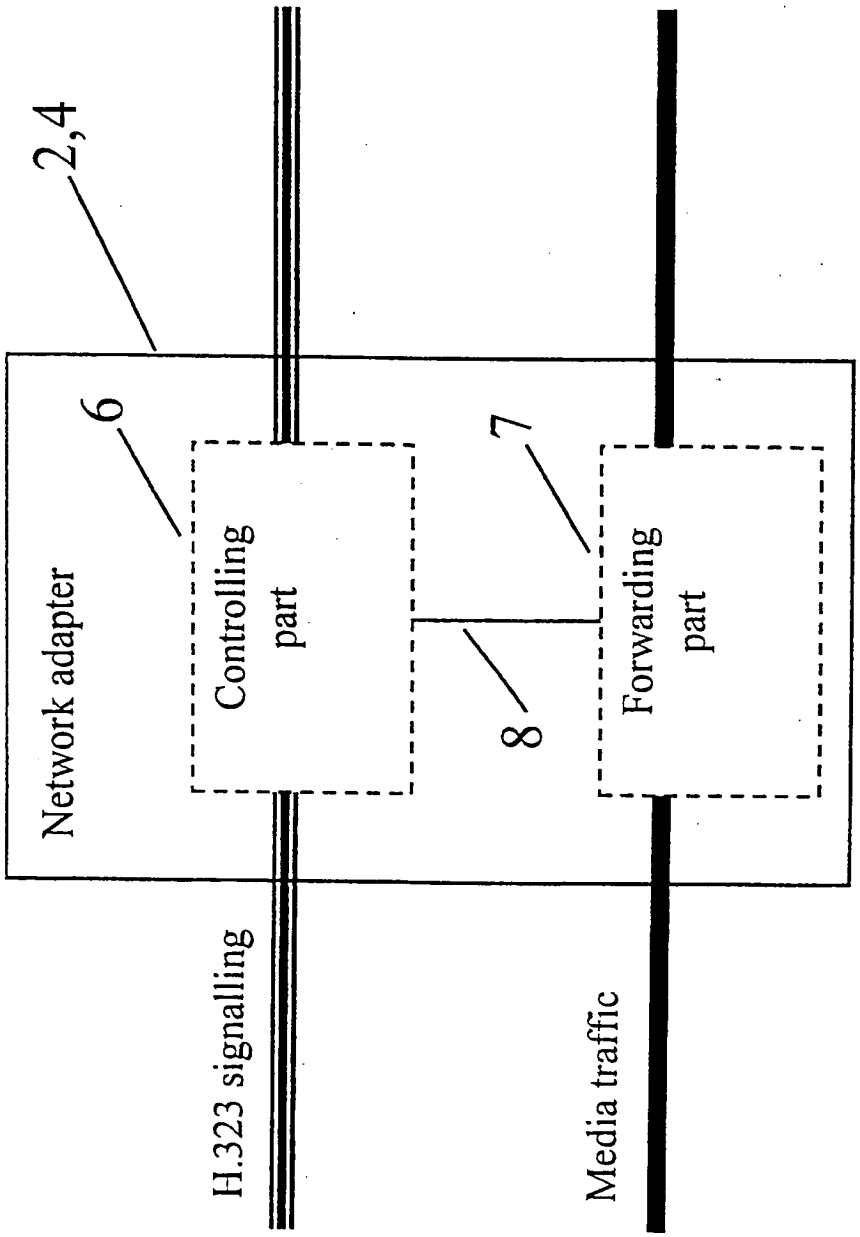

2,4
Network adapter
6
Controlling part
7
Forwarding part
8
H.323 signalling
Media traffic

Fig. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 00/00336

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/64, H04L 29/06
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 9817048 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY), 23 April 1998 (23.04.98), page 1, line 7 - page 3, line 12; page 7, line 2 - page 9, line 33, claims 1-23	1-9
Y	US 5958015 A (Z.DASCALU), 28 Sept 1999 (28.09.99), see the whole document	1-9
P,Y	EP 0967764 A2 (SIEMENS INFORMATION AND COMMUNICATION NETWORKS), 29 December 1999 (29.12.99), column 1, line 13 - column 4, line 35, claims 1-20	1-9

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 January 2001	05 -02- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Roger Bou Faisal/LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 00/00336

A. CLASSIFICATION OF SUBJECT MATTER

IPC7: H04L 12/64, H04L 29/06
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC7: H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 9817048 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY), 23 April 1998 (23.04.98), page 1, line 7 - page 3, line 12; page 7, line 2 - page 9, line 33, claims 1-23	1-9
Y	US 5958015 A (Z.DASCALU), 28 Sept 1999 (28.09.99), see the whole document	1-9
P,Y	EP 0967764 A2 (SIEMENS INFORMATION AND COMMUNICATION NETWORKS), 29 December 1999 (29.12.99), column 1, line 13 - column 4, line 35, claims 1-20	1-9

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 January 2001	05 -02- 2001
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Roger Bou Faisal/LR Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/NO 00/00336

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 9837664 A2 (NORTHERN TELECOM LIMITED), 27 August 1998 (27.08.98), page 2, line 8 - page 3, line 18, claims 1-10, cited in Application	1-9
A	EP 0910197 A2 (LUCENT TECHNOLOGIES INC.), 21 April 1999 (21.04.99), page 2, line 35 - page 3, line 14, abstract	1-9
A	US 5802058 A (P.HARRIS ET AL.), 1 Sept 1998 (01.09.98), claims 1-5, abstract, cited in Application	1-9
A	US 5898830 A (R.WESINGER, JR. ET AL.), 27 April 1999 (27.04.99), claims 1-10, abstract, cited in Application	1-9

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/NO 00/00336

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9817048 A1	23/04/98	AU 4630597 A	11/05/98
		EP 0932972 A	04/08/99
		GB 9621524 D	00/00/00
US 5958015 A	28/09/99	AU 4992097 A	22/05/98
		EP 1010091 A	21/06/00
		WO 9819250 A	07/05/98
EP 0967764 A2	29/12/99	AU 1140500 A	08/05/00
		WO 0023432 A	27/04/00
WO 9837664 A2	27/08/98	EP 0962073 A	08/12/99
		GB 2322516 A	26/08/98
		GB 9703679 D	00/00/00
EP 0910197 A2	21/04/99	JP 11167538 A	22/06/99
US 5802058 A	01/09/98	AU 714600 B	06/01/00
		AU 2366497 A	11/12/97
		CA 2200120 A	03/12/97
		EP 0812089 A	10/12/97
		JP 10093638 A	10/04/98
US 5898830 A	27/04/99	US 6052788 A	18/04/00